RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: GRC-T01

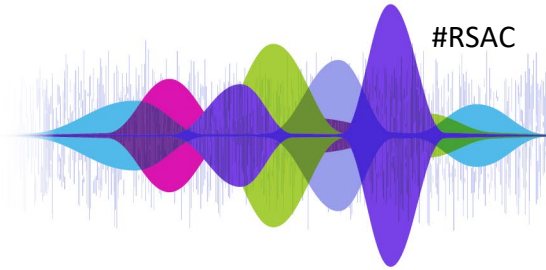
Policy Pyramid to Deployment: A Community Approach to Deploying Security

Stephanie Gass

Sr. Director of Information Security
Center for Internet Security
https://www.linkedin.com/in/stephanieraegass/

Kennidi Ortega

Sr. Information Security Analyst
Center for Internet Security
https://www.linkedin.com/in/kennidiortega/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

All trademarks, logos and brand names are the property of their respective owners. All company, product and service names used in this presentation are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement by the Center for Internet Security, Inc. Opinions of the presenter are their own and mention of any product or organization by name should not be considered an endorsement by the Center for Internet Security, Inc.

“Center for Internet Security is a registered trademark of Center for Internet Security, Inc. (c) 2025 Center for Internet Security, Inc.”

Overview

- Policy Pyramid
- Policy & Implementation
- Leveraging GenAI to Simplify Policy Implementation & Communication
- Ensuring Policy Adoption & Success

RSAC 2025 Conference

Policy Pyramid

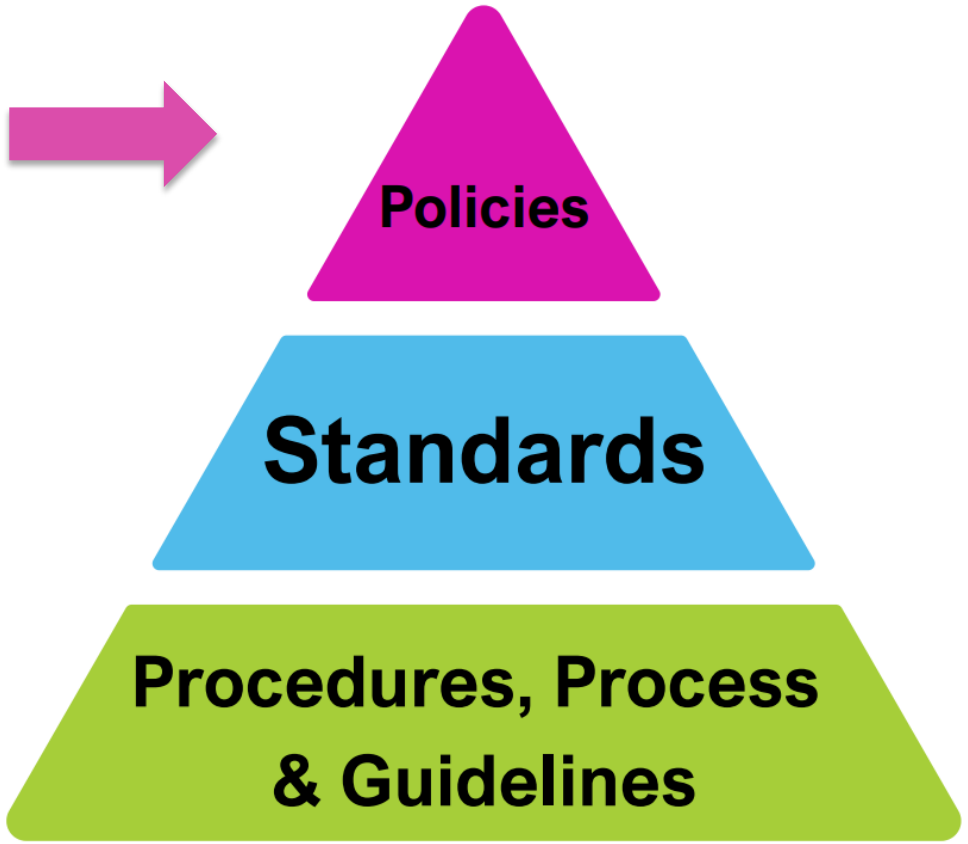
Policy Pyramid

Why a Policy Pyramid?

- What Governs You?
- What are my “Crown Jewels”?
- What staff do I have available to me and what are their skills?

Policy Pyramid – Policies

Policy Pyramid

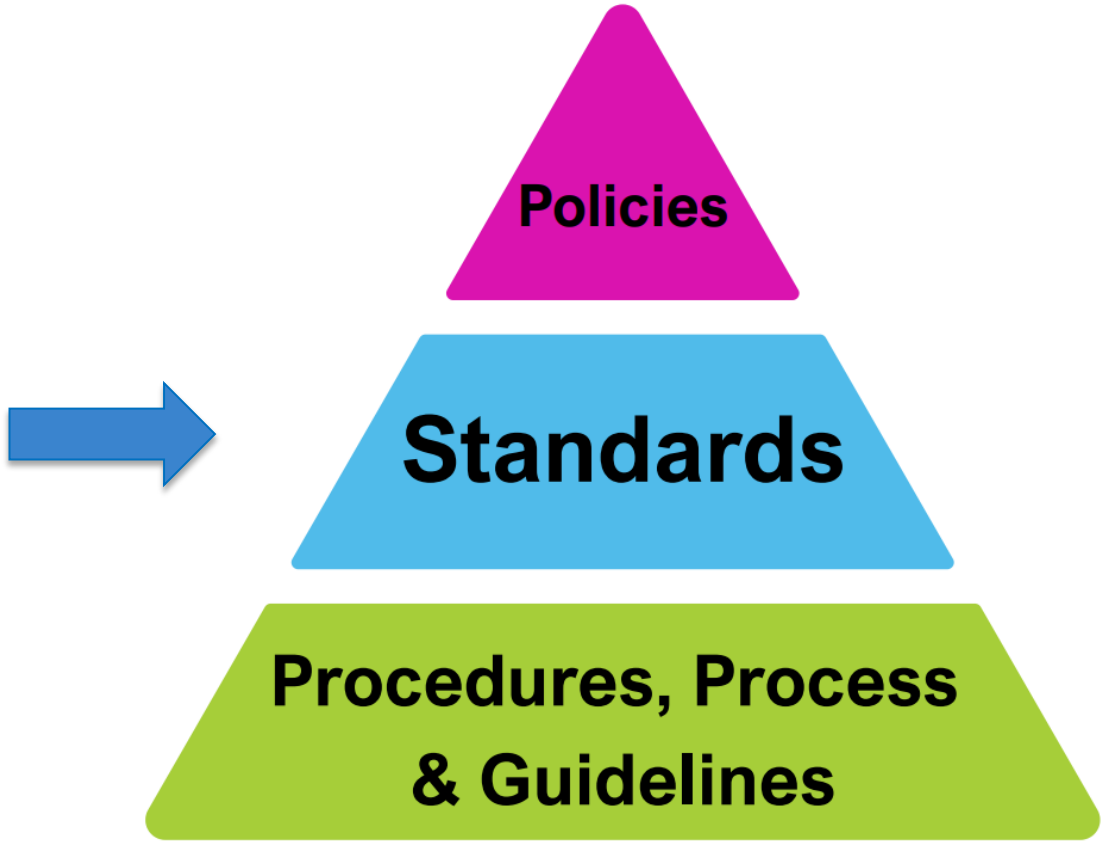


Policies

- Highest Level
- Based on What Governs You

Policy Pyramid – Standards

Policy Pyramid



Standards

- Creating the Foundation
- What are my "Crown Jewels"?
  - Protecting

Policy Pyramid – Procedures, Process & Guidelines

Policy Pyramid

Procedures, Process & Guidelines

- Understanding the "How"

Policy Pyramid – Implications

- Why security teams must collaborate to ensure policies are actionable.
  - The "Why"
- Each level supports implementation
  - Policies define direction
  - Standards define measurable security controls
  - Procedures, Process, & Guidelines provide recommendations + step-by-step execution

RSAC™ 2025 Conference

Policy & Implementation

Business & Security Considerations

- Challenges in Policy Adoption:
  - How security and business teams negotiate usability and security
  - Impact on productivity
  - Technical complexity
- How business requirements shape security decisions
- Example: MFA Deployment
  - Adjusting MFA requirements based on risk level and user role

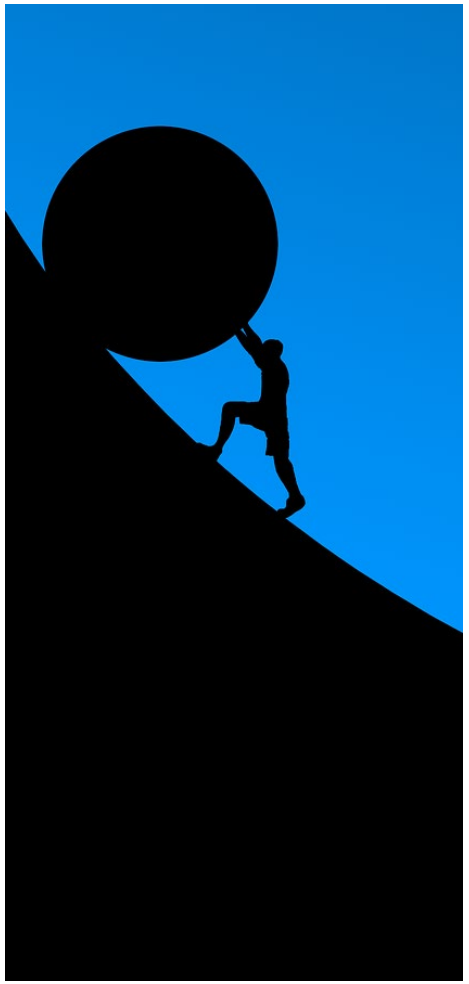
Policy in Action – Real-World Example

Policy Pyramid

MFA Example

- Policy
  - Defines the need for MFA and sets the high-level expectation
- Standard
  - Work together to determine technical requirements
- Procedure, Process, & Guidelines
  - Converts the standard into actionable steps for users, IT admins, and security teams
  - Ensures system-wide enforcement

Policy in Action – Overcoming Challenges

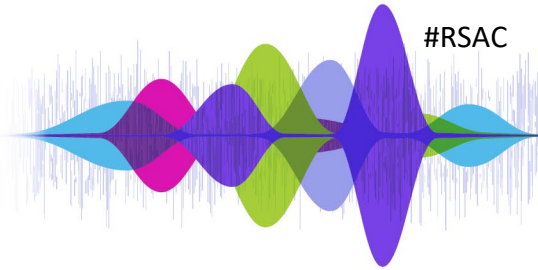


- User resistance & training
  - Employees perceive MFA as an inconvenience
- Technical barriers & workarounds
  - Legacy systems that don't support MFA
- Business constraints
  - MFA enforcement for external contractors
- Collaboration in refining the process
  - How we work together to adjust MFA policies based on user feedback and business needs

The Bridge Between Policy and Implementation

- Why does the gap exist?
  - Policies set expectations, but enforcement requires execution
- Collaboration is **crucial** in security policy implementation
- Policies only work when they are implemented *effectively*
- Many organizations struggle to translate frameworks into actionable security measures

Policy & Implementation – Security Gaps



- Gaps in Policy Coverage
  - Emerging threats (AI-powered phishing)
- Conflicting Policies or Priorities
  - Security policies can clash with operational efficiency
- Implementation Blind Spots
  - Employees adopting unapproved AI tools
- False Sense of Security
  - Passing audits ≠ real security

Turning Policy into Action – Bridging the Gap

- Policies exist, but how do teams actually follow them?
- Bridge the gap between policy and execution
  1. Identify who needs to be involved
  2. Compliance enforcement
  3. Clear instructions
  4. Best practice for cross-team collaboration
     - Techniques for ensuring policies align with business objectives **and** security goals
       - *"Why?"*
     - How security teams, IT, and leadership work together to ensure compliance

RSAC™ 2025 Conference

Leveraging Gen AI to Simplify Policy Implementation & Communication

AI's Role in Streamlining Policy Execution

- Translate complex requirements into plain language
  - Be **specific**!
- How does AI help different levels of the Pyramid:
  - GRC: Analyzing frameworks and drafting policies.
    - AI-assisted policy analysis and drafting
  - Operations: Mapping policy requirements into technical procedures.
    - AI-generated compliance mappings

NIST Example – Clear Communication

Prompt

You are a cybersecurity professional creating a document for a non-technical program manager. Review NIST SP 800 171 R3 for each item in the security requirements provide the following information:

Control Number (e.g., 3.1)
Control Name (e.g., 03.01.01)
Control Coverage (adjust Account Management)
A simple description of the proceeding items.
An itemized list of simplified items required to meet the control including information from each bullet point.

Take time to review the list you have created with the target audience of a non-technical program manager in mind and adjust where necessary before providing me the answers.

Please do this for all 17 requirements. Please do each requirement in order from 3.1 - 3.17 including each sub item 03.01.01 - 03.17.03 and any itemized lists below those sub items.

Answer

Control 3.1: Access Control

Control Number: 3.1
Control Name: 03.01.01 - Limit System Access
Control Coverage: Adjust Account Management
Description: Ensure only authorized users can access the system and its data.
Simplified Requirements:

1. Identify and document authorized users.
2. Implement mechanisms to restrict access to authorized users only.
3. Regularly review and update access permissions.

Control Number: 3.1
Control Name: 03.01.02 - Control Internal System Access
Control Coverage: Adjust Internal Access
Description: Manage access within the system to ensure users can only access what they need.
Simplified Requirements:

1. Define and document internal access controls.
2. Implement access controls to limit internal access.
3. Regularly review and update internal access permissions.

Control 3.2: Awareness and Training

Control Number: 3.2
Control Name: 03.02.01 - Security Awareness Training
Control Coverage: Adjust Training Programs
Description: Ensure all users are aware of security policies and procedures.
Simplified Requirements:

1. Develop and provide security training to all users.
2. Ensure training covers key security policies and procedures.
3. Regularly update training materials to reflect current threats and policies.

Mapping Example

Do I need a prompt?

Map the CIS Critical Controls v8.1 to NIST SP800-53

Copilot

Mapping the CIS Critical Controls v8.1 to NIST SP800-53 involves aligning the specific controls and safeguards from CIS with the corresponding security and privacy controls in NIST SP800-53. Here are some key points to consider:

1. **Governance and Risk Management**:
   - **CIS Control 1 (Inventory and Control of Enterprise Assets)** maps to **NIST SP800-53 CM-8 (Information System Component Inventory)**.
   - **CIS Control 2 (Inventory and Control of Software Assets)** aligns with **NIST SP800-53 CM-7 (Least Functionality)**.

Can you provide a more detailed mapping?

Copilot

Certainly! Here is a more detailed mapping of CIS Critical Controls v8.1 to NIST SP800-53:

Governance and Risk Management

- **CIS Control 1 (Inventory and Control of Enterprise Assets)**:
  - **NIST SP800-53 CM-8 (Information System Component Inventory)**: Ensures all components are inventoried and managed.
- **CIS Control 2 (Inventory and Control of Software Assets)**:
  - **NIST SP800-53 CM-7 (Least Functionality)**: Ensures only necessary software is installed and active.

No, You can just iterate

How to measure the effectiveness of the detailed mapping?

Copilot

Measuring the effectiveness of the detailed mapping between CIS Critical Controls v8.1 and NIST SP800-53 involves several key steps:

1. Define Metrics and KPIs

- **Compliance Rate**: Measure the percentage of controls that are fully implemented and compliant.
- **Incident Reduction**: Track the number of security incidents before and after implementation.
- **Audit Results**: Evaluate the findings from internal and external audits.

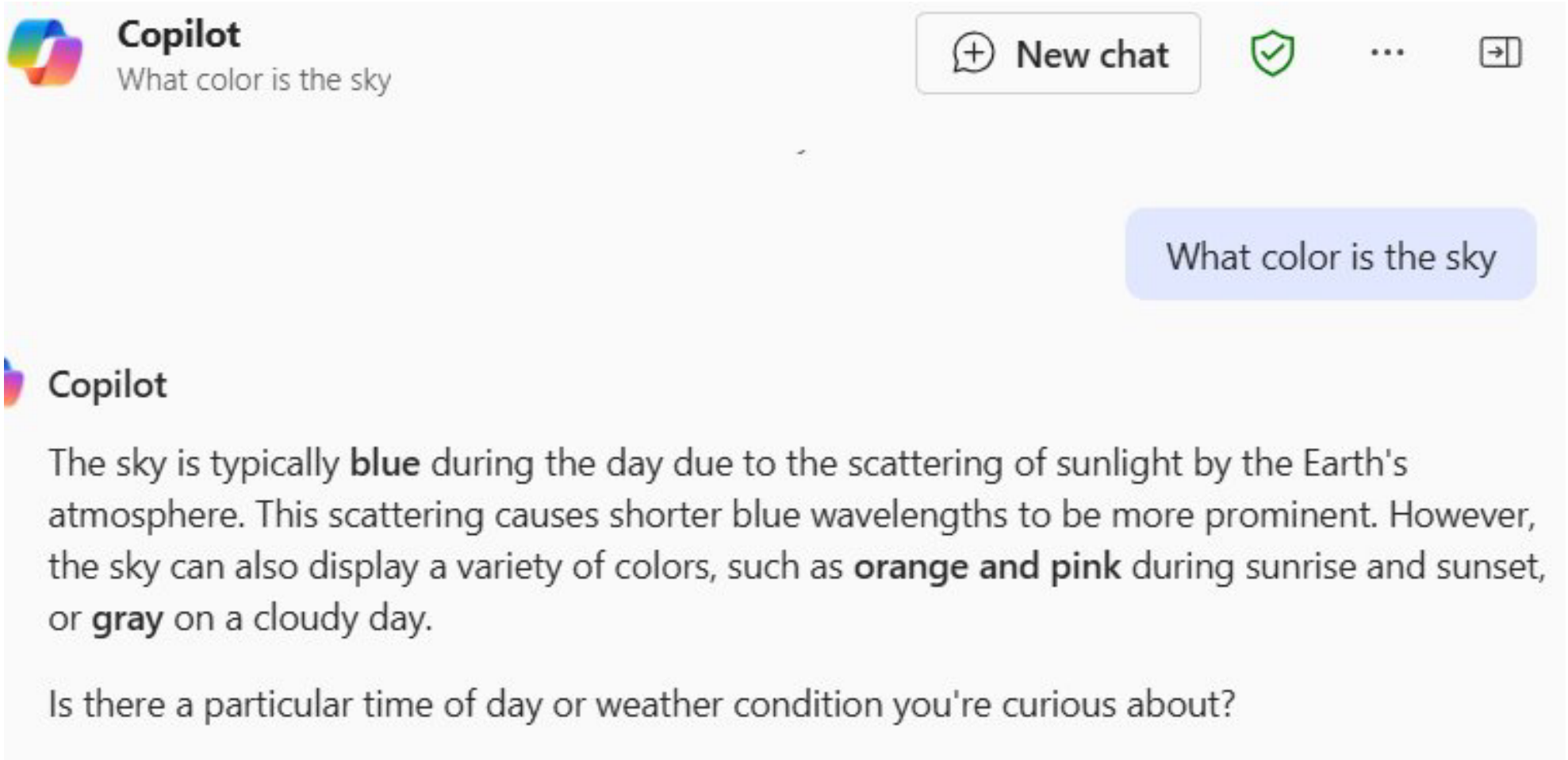
2. Conduct Regular Assessments

- **Gap Analysis**: Identify gaps between current practices and the mapped controls.
- **Vulnerability Assessments**: Regularly scan for vulnerabilities and measure the reduction in vulnerabilities over time.

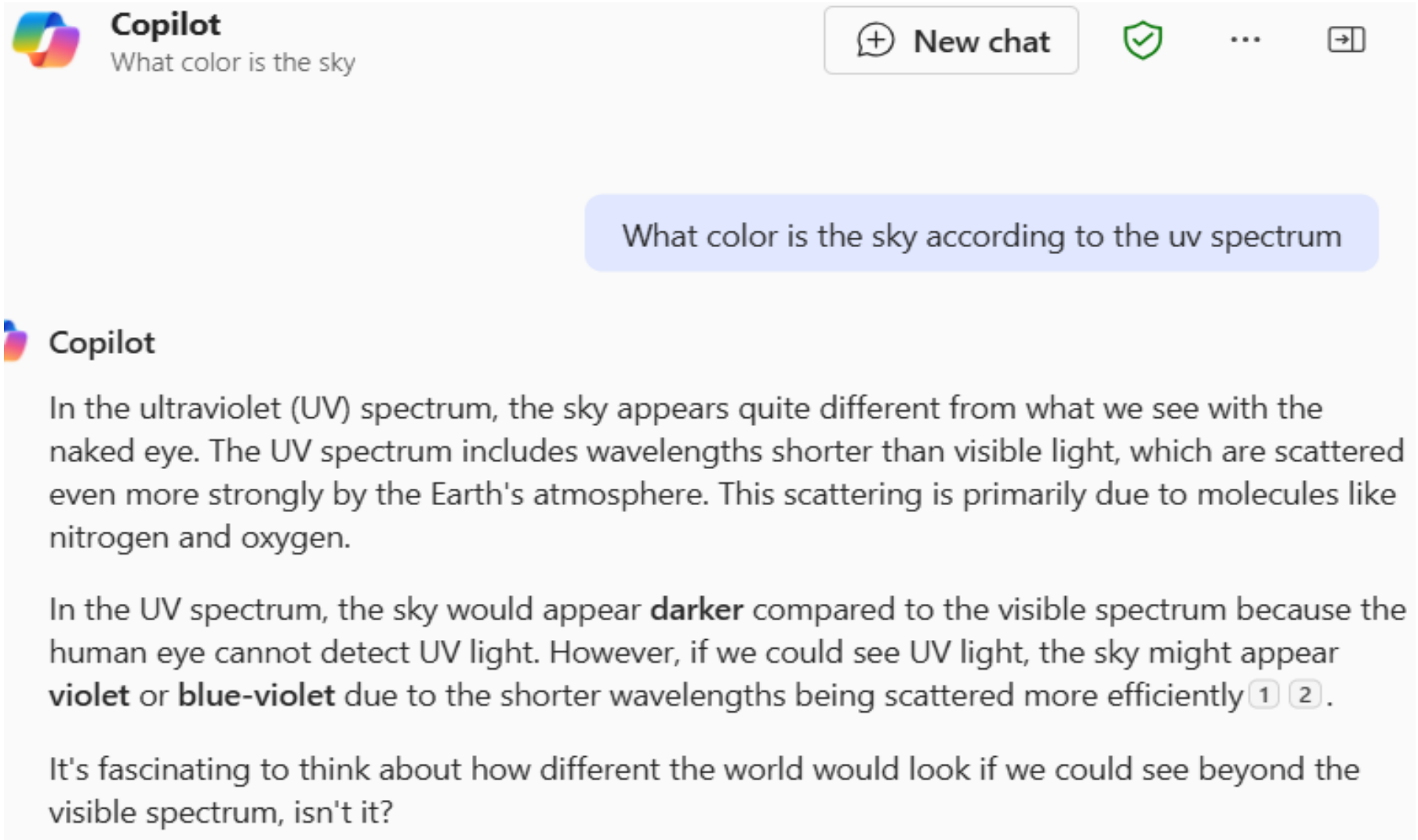
AI Limitations in Policy Implementation

- AI does not know your environment!
  - Governance
  - Crown Jewels
  - Personnel

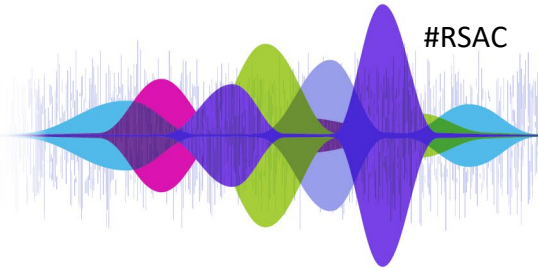
Example – No Context


Copilot
What color is the sky
New chat
What color is the sky
Copilot
The sky is typically **blue** during the day due to the scattering of sunlight by the Earth's atmosphere. This scattering causes shorter blue wavelengths to be more prominent. However, the sky can also display a variety of colors, such as **orange and pink** during sunrise and sunset, or **gray** on a cloudy day.
Is there a particular time of day or weather condition you're curious about?

Example – Context


Copilot
What color is the sky
New chat
What color is the sky according to the uv spectrum
Copilot
In the ultraviolet (UV) spectrum, the sky appears quite different from what we see with the naked eye. The UV spectrum includes wavelengths shorter than visible light, which are scattered even more strongly by the Earth's atmosphere. This scattering is primarily due to molecules like nitrogen and oxygen.
In the UV spectrum, the sky would appear **darker** compared to the visible spectrum because the human eye cannot detect UV light. However, if we could see UV light, the sky might appear **violet** or **blue-violet** due to the shorter wavelengths being scattered more efficiently 1 2 .
It's fascinating to think about how different the world would look if we could see beyond the visible spectrum, isn't it?

Human vs AI-Driven Decision Making



- Human Strengths:
  - Contextual awareness
  - Ethical considerations
  - Flexibility in unique scenarios
- AI Strengths:
  - Speed & Automation
  - Pattern recognition in datasets
  - Consistency in enforcement
- Strike the right balance!
  - AI supports *enforcement*, but humans drive *strategic decisions*

RSAC 2025 Conference

Ensuring Policy Adoption & Success

Making Policies Stick – Ensuring Adoption

- Policies exist, but teams don't always follow them.
- Avoid common pitfalls
  - Policies that are too vague or too rigid
  - Lack of training and awareness leads to policy failures
  - Policies that never leave the documentation phase

Making Policies Stick – Ensuring Adoption (Cont.)

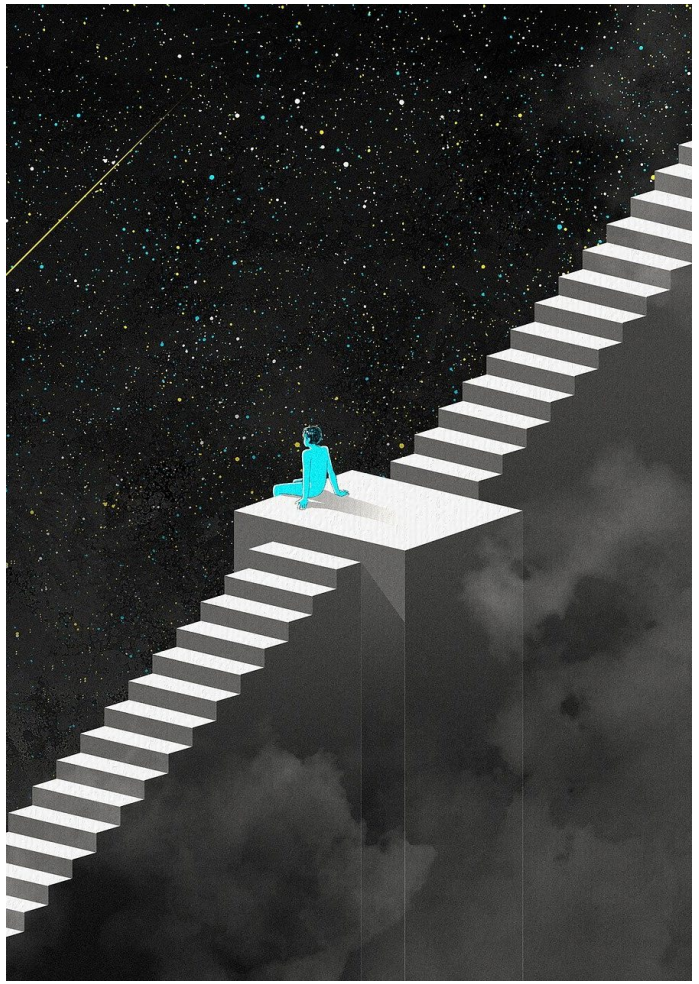
- Ensuring adoption through practical steps
  - Provide training and clear, actionable documentation
  - User real-world scenarios to test procedures
  - Regularly review and refine policies based on feedback
  - Use AI for mapping policy-to-operations efficiently

Revisiting the MFA Example

1. Policy Level
2. Standard Level
3. Procedure, Process, & Guidelines Level
4. Challenges & Security Gaps
5. Key Takeaways

The Future of Policy-Driven Security

- Where are security policies heading?
  - AI-driven policy management
  - AI-assisted compliance monitoring
  - Greater automation of enforcement with security tools



Tips for Success

- Make security policies actionable and effective!
  - Align policies with business objectives
- Ensure clear documentation and communication
- Continuously improve & adapt
  - Regularly update policies to reflect new threats

Apply What You've Learned

- 30 Days
  - Assess one security policy
  - Start a conversation
- 90 Days
  - Map policies to the Policy Pyramid
  - Pilot AI or Automation for Compliance
  - Conduct a Security Gap Analysis
- 180 Days
  - Improve Security Training & Awareness
  - Measure Policy Effectiveness

Security policies are only effective when *enforced* – start bridging the gap <u>today</u>!

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you!